eDIS – Electronic Diploma Integrity Service

Paul-Cristian VASILE, Andreea DINU
National Institute for Research and Development in Informatics - ICI Bucharest
paul.vasile@ici.ro, andreea.dinu@ici.ro

Abstract: This paper presents the eDIS - Electronic Diploma Identity Service application, a platform that enables validation and verification services for diplomas issued by entities in the educational environment. The main technologies, the implemented functionalities and the use cases are also highlighted in this paper. It also analyses the current state of digitalisation in the field in which the eDIS application falls, both nationally and internationally. At the same time, similar solutions were examined. For conclusions, opportunities for improvement and expansion were outlined.
Keywords: Blockchain, Self-sovereign Identity, Digital Identity, Verifiable Credentials

INTRODUCTION

In recent years, the evolution of emerging technologies had a significant impact on the way our society operates. With the release of new technologies, each activity sector improved their business models, workflows and interaction methods with modern and simplified procedures. The automation and replacement of operating procedures have reduced the costs and effort required to carry out daily tasks. These technologies, like quantum computing, blockchain empowered digital credentials, verifiable identities and so on, have become of major interest in research and educational areas. At educational level, especially in the academic space, in addition to the tendency of introducing the technologies of the future in the current curriculum, we can also mention the digitalization of specific management procedures. Most of the existing universities have digitalized certain key operating procedures such as the enrolment or the certification process, so that the experience of the students became easier and more accessible. Recently, in the university environment, a considerable evolution in terms of digitalization was noticed, many specific management procedures being replaced by online versions. The main problem regarding the issuance and verification of diplomas is their forgery, because during the past few years, many cases and attempts of fraud were detected. Given the recent technological trends, blockchain technology is a viable solution for verifying authenticity, especially in the case of diplomas, improving the traditional processing and response time. The implementation of an IT ecosystem that offers the possibility to verify and authenticate diplomas in a secure and isolated environment brings significant added value in the digital identity environment and lays the foundations of a verification ecosystem that can help build the future of digital solutions.

THE CURRENT SITUATION

The interest in blockchain technology can be observed both internationally and nationally. Currently, there are multiple initiatives to integrate this technology in many areas, including education.

At national level, within the University of Timișoara there is a postgraduate study program called „Blockchain Entrepreneurship" (University of Timisoara), with the main purpose of presenting the fundamentals of blockchain technology, application areas, development initiatives and funding resources for future projects. Also, Prof. Dr. Carmen Holotescu, together with Victor Holotescu, PhD student in blockchain, implemented the RO-Certs system, which allows the registration of diplomas, certifications and electronic portfolios on the blockchain. The implementation of the solution was capitalized through a pilot project for issuing honorary diplomas to students, an initiative organized by the University of Timisoara and INACO (INACO, 2021).

Also, the Executive Blockchain Laboratory (Executive Blockchain Laboratory, 2021), within the National Institute for Research and Development in Informatics - ICI Bucharest, offers the course „Blockchain Technology: Application and Innovation of Transformational Business", which aims to present opportunities for the development of blockchain solutions in the business environment. This course is an opportunity to get knowledge from nationally and internationally recognized entities in the blockchain field, from the private and academic field (e.g. MODEX, TAILPATH , Action4Value , Old Dominion University, Vienna University of Economics and Business). The certification diploma for this course is registered on a piloted blockchain and the participants are able to view the registered data through a QR code, which is distributed on the digital and physical version of the diploma.

At international level, under the coordination of the European Commission, the European Blockchain Partnership has been set up. Following this partnership, the first European blockchain network – EBSI (EBSI, 2021) was developed. The main objective of the partnership is to create a workgroup at European level in order to develop applications that facilitate European services using decentralized systems. Since 2020, EBSI is a functional blockchain network with operating nodes in over 29 European countries, currently providing support for 4 main use cases:

- Self-Sovereign Identity - implementing a model that allows citizens to create and own a valid digital identity that can be verified anywhere in Europe.
- Diploma - citizens obtain digital accreditations of educational documents, saving their verification and authentication costs.
- Notarization - citizens can prove the integrity and provenance of documents more easily.
- Data sharing - secure data sharing between the customs and tax authorities of the European Union.

From 2019, Romania became a member of the European Blockchain Partnership, contributing to the development and implementation of EBSI. The EBSI infrastructure complies with European Union regulations (GDPR, eIDAS, etc.), and it's architecture is based on three layers (EBSI, 2021):

- Infrastructure layer - provides generic capabilities and connectivity to blockchain networks.
- Storage layer - encompasses blockchain storage protocols currently supported by EBSI.
- Basic services - includes APIs that allow users to develop applications that comply with the principles defined and approved by the European Blockchain Partnership.

BASIC CONCEPTS

In the development of the eDIS aplication two important concepts that defined the architecture and the methods of interaction

between users were followed: blockchain technology and self-sovereign identity.

Self-sovereign identity (SSI)

A digital identity can be defined as a snapshot of the current identity details of a person, a company - or any entity. Each digital identity is created to serve a specific purpose and may contain personal details such as name, surname, date of birth, social identification number, etc., as well as specific data used by the consumer service, such as height, weight, address, banking account, etc. For each existing entity, several digital identities can be created to be used for different purposes. A secure digital identity must take into account two aspects (Der, Jahnichen, & Surmeli, 2017):

- confidentiality - only authorized entities can access a certain digital identity, and the information contained is available only with the consent of the entity (owner) defined by that identity.
- trust - refers to the correctness and integrity of the data found in the digital identity, which provides a certain degree of validity assurance.

Thus, to ensure these two requirements, the concept of self-sovereign identity (SSI) was introduced, which allows the exclusive management of all digital identities to be done by the owner. This technology offers three essential elements: individual control, security and complete portability. All external controls are eliminated, so that the user owns and manages the data without the need for an external party to centralize the identities for all entities. Digital identity is independent of any external technology and is controlled only by the owner, who authorizes and creates these identities (Stokkink, 2018).

Christopher Allen, a specialist in security and cryptography, defined 10 basic principles of SSI architecture (Allen, 2016):

- Existence - the user must exist as an entity in society. Digital identity is defined based on the identified identity of the user in society such as identity card, birth certificate, etc. It serves as a support in identifying the user, providing the necessary details for each existing scenario.
- Control - the user is the only one who can manage his digital identity. It has full rights to it's digital identity (deletion, update, etc.), even if the validity of the data is ensured by algorithms and mathematical methods.
- Access - the user must have access to his personal identity data and have the ability to decide what actions can be taken on the identity.
- Transparency - the algorithms and systems used to manage the digital identity network must be known, valid and public.
- Persistence - the identity must be valid for a long period of time, either until the identity data is no longer valid or the user no longer wants that identity. Given the rapid evolution of the Internet, there is a possibility that the way of creating digital identities may no longer be compatible and then it is necessary to have an option to update the digital identity to an accepted format.
- Portability - the information of a digital identity and the services used must be portable and accessible, so that the user always remains in control of his own identity.
- Interoperability - it is important that digital identity identification systems work globally and recognize all types of digital identities.
- Consent - the user must agree to share or access the digital identity. Regulations regarding the safety and privacy of the user must be applied and monitored.
- Minimization - a user's digital identity must contain only the data necessary for identification in a certain context. For example, to identify themselves when attending an event, the organizers may ask for data such as first and last name, so that no other data from the identity has to be disclosed.
- Protection - user rights must be respected, so whenever a conflict may arise between the user's digital identity and the interests of the network that

manages the identities, the user's rights must always be prioritized. This is ensured by the authentication method, performed independently, using algorithms that do not depend on the network infrastructure.

To ensure the integrity, authenticity and persistence of data, self-sovereign identity management systems are based on blockchain technology.

Blockchain technology

Blockchain is a technology based on the concept of distributed digital information. This technology can be defined as a chain of data records, stored in blocks, which cannot be modified later (immutable), but only added to new versions of this blocks. Blockchain technology is distributed, consisting in nodes containing a copy of the data and is cryptographically validated using hash functions. A blockchain uses two types of elements (National Institute of Standards and Technology, 2018):

- Transactions - actions created by participants in this kind of networks
- Blocks - transaction records, which must ensure the correct order of transactions and their non-alteration.

Over time blockchain technology has been adopted in many of the essential sectors, having a major impact on the development of activities and quality sensible services such as: health, finance, vehicle communication, IoT, education, e-government and so on. There are three categories of blockchain (National Institute of Standards and Technology, 2018) :

- public - anyone can participate in the public blockchain, without needing any prior permission.
- private - in the private blockchain you can participate only by invitation, being managed by a single entity; participants ask the permission to search and write on the blockchain network.
- hybrid - in the hybrid blockchain, there is control over transactions and participants, only the actions that are decided by mutual agreement between the participants being public.

From the security and technological point of view, the information contained in the blockchain network is stored in blocks, which are then cryptographically linked. As you want to add new data, they are filled in a data chunk that will later be added to the chain, thus maintaining the chronological order. The most important aspects that blockchain addresses, representing the major advantages it offers, are (National Institute of Standards and Technology, 2018):

- peer to peer communication - a way of direct interaction between communication participants
- decentralization - data is recorded on all nodes in the network, each node having an identical copy, thus, in the event of a cyber attack, the data is instantly recovered
- security - currently, blockchain technology is considered theoretically imune to DDoS attacks, because of the complexity of the required attack
- audit - the ability to navigate through all the existing blocks in the network, provides chronologycal traceability of each change.

Blockchain technology can be introduced when systems have the following requirements (National Institute of Standards and Technology, 2018):

- numerous and distributed participants;
- the flows of activities are of transactional type;
- the need for a real-time monitoring system of activities;
- the need to visualize the origin of digital assets and transactions, what is needed distributed to all participants.

ARCHITECTURE AND TECHNICAL DETAILS

eDIS is an informatic system that verifies and confirms the authenticity of a diploma corelated with the identity of a user by making use of verifible credentials. For a better understanding

regarding the arhitecture we will define the main elements of the system:

- DID - distributed identifier of the cryptographically generated / registered user. Each DID is associated with a document DID, which is a set of user-defining data, such as public keys, that are used to authenticate and demonstrate the authenticity of the entity (W3C, 2021).
- Credential - represents a set of data requested in a certain context (for example, a credential can consist of name, surname and age for joining a club, with a permitted age over 18).
- Connection - the relationship between a user and an entity that supports the use of SSI as a method of authentication and identification.
- Proof (proof) - the request by an entity to present a credential that contains certain specified data.

We will explain the eDIS arhitecture based on the following figure:

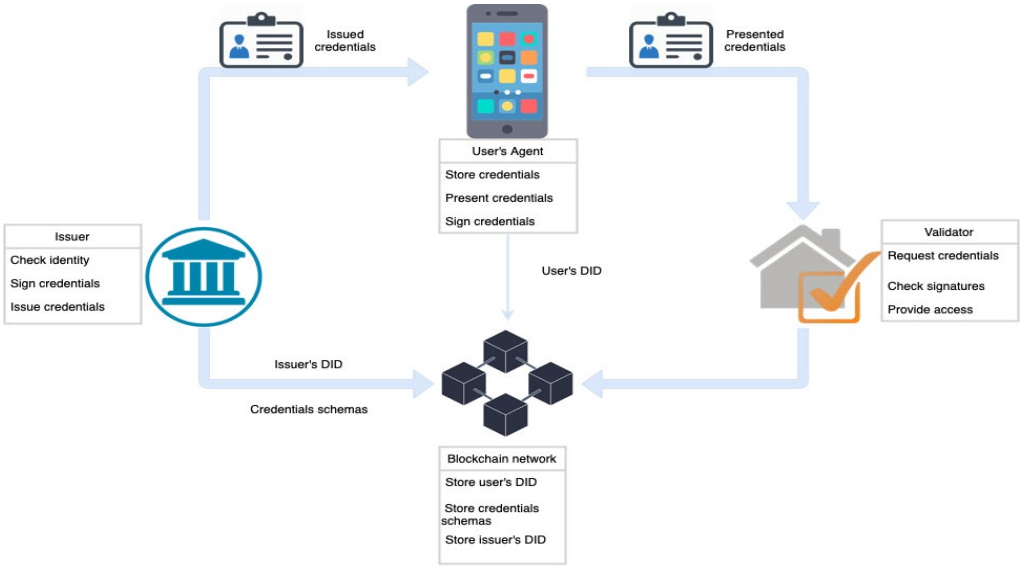

Fig. 1: *eDIS architecture*

As we can see in the figure above, there are four main actors that have different roles in the whole process of issuing and presenting credentials for validation:

1. Blockchain network – it stores all the users DIDs and credential schemas for further verification and validation.
2. Issuer – is the entity that certifies the identity of the user by creating a secure communication channel, signing the credential and issuing it to the user.
3. User – Stores the issued credential in his electronic wallet in order to present it whenever it is needed.
4. Validator – is the entity that requests a proof check and verifies that the credential was not modified using blockchain network.

In the development of the eDIS application three important projects from the Hyperledger family were used: Hyperledger Indy for the blockchain network, Hyperledger Aries for the interaction between agents and blockchain network and Hyperledger Ursa for the digital signatures and other criptoghrapic operations.

In our diploma case, the issuer can be any authorazed entity that has the right to issue a diploma, for example national universities. The users are represented by the students which use their digital wallet for interacting with the issuer. The application is interoperable with any digital wallet and we tested it with several wallets like Trinsic, Lissy and others. The validator can be any institution that needs to verify the user diploma before other further procedures.

SIMILAR SOLUTIONS

Over time, there have been numerous initiatives to introduce various applications that are based on the decentralized concepts of blockchain technology in the education system. One of the first similar applications in this field is Blockcerts, which allows the verification and validation of official certificates using blockchain. It's implementation is based on a series of modules, which together ensure the creation, issuance, viewing and verification of certificates (Oliver, Moren, Pietro, & Benitez, 2018).

Another application worth mentioning is BCert. It aims to verify and distribute digital certificates, implementing smart contracts concepts. Three types of users are defined: the issuer (universities or training centers), the consumer (students, employers or academic institutions) and the accreditation body. This application gives the issuer control over the addition, issuance and viewing of study diplomas. Consumers have the possibility to view the accreditations and to approve / disapprove their publication. Ethereum is the blockchain network that underlies the implementation of the BCert application (Elva & Besnik, 2020)

SmartCert is an application that aims to facilitate the verification of diplomas and certificates of future employees. In order to be able to establish the authenticity of diplomas, it is necessary for the holder of the document to share the related hash with the companies interested in hiring him (Omar, Saleh, Ghazali, & Ehsan, 2020).

Educhain, in addition to functionalities similar to the eDIS application, has also developed an „academic passport" that stores all students' achievements, which include means of graduation, exam marks and awards (Liu, et al., 2021).

We also mention other significant initiatives in the field such as: EduCTX (Trukanovic, Holbl, Kosic, & Kamisalic, 2018), UZHB (Gresch, Rodrigues, Sheid, & Kanhere, 2018),UNIC (The University of Nicosia, 2016), Cerberus (Tariq, Hag, & Ali, 2019).

DEVELOPMENT OPORTUNITIES

The concepts and technologies used for the development of the eDIS - Electronic Diploma Integrity Service application can be extended to the simplification of other procedures in the educational system such as:

- Issuance of student certificates - on the same principle, credentials can be created that can be presented wherever data attesting student status is required.
- Examination credentials - a credential can be issued with the necessary data for participation in the exam, with the possibility of introducing conditions, such as a student can not participate in the exam if he does not have at least five attendances.
- Issuing the credential corresponding to the student card - which is extremely requested when it comes to discounts offered on public transport.

As an impact at national level, the implementation of the eDIS application within the important universities in the country can facilitate the development of a national blockchain network, on which decentralized concepts can operate. The benefits of implementing the eDIS application can be achieved through a funding program, which supports national research and development projects. This, following the necessary improvements, it can be tested as a pilot project, building partnerships between universities and accreditation centers.

At European level, it can operate on the EBSI blockchain network, so the visibility of the application, as well as of Romania, would increase and partnerships could be generated for the development and standardization of procedures at European level, according to EU rules. At the same time, there are funding programs for the development and introduction of blockchain technologies in the private, but especially public sectors.

CONCLUSIONS

The eDIS - Electronic Diploma Identity Service application is a new and innovative mechanism for issuing, verifying and validating diplomas. At the same time, it introduces concepts for verifying digital identity by issuing credentials and storing them in users' electronic wallets.

Opportunities for the development of the concepts presented by the application can significantly contribute to the current digitalization initiatives at national level and alignment with the Member States of the European Union. Regarding the technologies used, their continuous development can create an environment for collaboration between important entities in Romania and can encourage the development of startups by involving them in working groups. The creation of a national blockchain network, as well as a network of decision-making entities can position Romania among the states with a mature level of digitalization, so that the country's visibility can increase and attract European funds. Also, by forming the development ecosystem of blockchain-based technologies and applications, other partnerships can be established in order to solve problems in other important sectors of activity such as the financial-banking sector, the transport sector, the government sector, the legal, etc.

At the same time, through the opportunity of collaboration between academia and the private / public environment, the emerging technologies and their applications can be introduced in the university's program, which will surely be the main object of interest in the next five years, thus preparing human resources for the development of current as well as future jobs.

REFERENCE LIST

INACO. (2021). *Planul INACO dedicat elevilor de 10 – PRIMELE DIPLOME PE BLOCKCHAIN DE RECUNOAȘTERE A PERFORMANȚELOR ȘCOLARE DIN ROMÂNIA.* Retrieved from www.inaco.ro: https://inaco.ro/planul-inaco-dedicat-elevilor-de-10-primele-diplome-pe-blockchain-de-recunoastere-a-performantelor-scolare-din-romania/

Executive Blockchain Laboratory. (2021). *Executive Courses.* Retrieved from www.executiveblockchainlaboratory.ro: https://www.executiveblockchainlaboratory.ro/executive-courses.php

EBSI. (2021). *EBSI Documentation.* Retrieved from www.ec.europa.eu: https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/EBSI

Der, U., Jahnichen, S., & Surmeli, J. (2017, December 5). Self-sovereign Identity – Opportunities and Challenges for the Digital Revolution. *Arxiv*, p. 5.

Stokkink, Q. P. (2018). Deployment of a Blockchain-Based Self-Sovereign Identity. *IEEE 2018 International Congress on Cybermatics 2018 IEEE Conferences on Internet of Things, Green Computing and Communications, Cyber, Physical and Social Computing, Smart, Computer and Information Technology.*

Allen, C. (2016, April 25). *The Path to Self-Sovereign Identity*. Retrieved from www.lifewithalacrity.com: http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html.

National Institute of Standards and Technology. (2018). *Blockchain Technology Overview.*

W3C. (2021). *Decentralized Identifiers (DIDs) v1.0 Core architecture, data model and representations.* Retrieved from https://www.w3.org/TR/didcore/#dfn-did-documents

Oliver, M., Moren, J., Pietro, G., & Benitez, D. (2018). Using blockchain as a tool for traking and verification of official degrees: business model. *29th European Regional Conference of International Telecommunications society (ITS). Towards a Digital Future: Turning Technology into markets.* Trento, Italy.

Elva, L., & Besnik, S. (2020). BCERT - A DECENTRALIZED ACADEMIC CERTIFICATE SYSTEM DISTRIBUTION USING BLOCKCHAIN TECHNOLOGY. *International Journal of Information Technologies & Security*, pp. 103-118.

Omar, S., Saleh, O., Ghazali, O., & Ehsan, R. (2020). Blockchain based framework for educational certificates verification. *Journal of critical Reviews*, 79-84.

Liu, Y., Li, K., Huang, Z., Li, B., Wang, G., & Cai, W. (2021). EduChain: A blockchain-Based Education Data Management System. *Blockchain Technology and Application* (pp. 66-81). Singapore: Springer.

Trukanovic, M., Holbl, M., Kosic, M., & Kamisalic, A. (2018). EduCTX: A blockchain based higher education credit platform. IEE Access, 5112-5127.

Gresch, J., Rodrigues, B., Sheid, E., & Kanhere, S. (2018). The proposal of a blockchain-based architecture for transparent certificate handling. *1 Workshop on blockchain and Smart Contract Technologies (BSCT)*, 189-196.

Tariq, A., Hag, H., & Ali, S. (2019). Cerberus: A blockchain based accreditation degree verification system. *arxiv:192.06812v1.*

The University of Nicosia. (2016). *Unic Blockchain Programs.* Retrieved from https://www.unic.ac.cy/blockchain/

University of Timisoara. (2021). *Blockchain Entrepreneurship*. Retrieved from https://blockchain-info.uvt.ro.